UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

In re: MGM Resorts International Data Breach Litigation

This document relates to: All actions.

Master File No. 2:23-cv-01480

(Consolidated for pretrial proceedings with Case Nos. 2:23-cv-1481, 2:23-cv-1537, 2:23-cv-1549, 2:23-cv-1550, 2:23-cv-1577, 2:23-cv-1698, 2:23-cv-1719, 2:23-cv-1777, 2:23-cv-1826, 2:23-cv-1981, 2:23-cv-2042, 2:23-cv-2064, 2:24-cv-81)

CONSOLIDATED CLASS ACTION

Case No. 2:23-cv-01480

CONSOLIDATED CLASS ACTION COMPLAINT

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs, Tonya Owens, Emily Kirwan, David Zussman, David Lackey, Michael Pircio, David Terezo, Ronald G. Rundell, Anita Johnson, Paul Zari, Michael Manson, Kyle Sloan, Michelle Righetti, Edgar Mejia, and DuJun Johnson ("Plaintiffs"), individually, and on behalf of all others similarly situated ("Class Members") allege the following against Defendant, MGM Resorts International ("MGM" or Defendant") based on personal knowledge as to themselves and on information and belief as to the other allegations derived from, among other things, the investigation of the undersigned counsel:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to prevent a cyberattack that resulted in Plaintiffs' and other similarly situated MGM consumers'—the Class Members'—sensitive information, including, upon information and belief, their full names, dates of birth, addresses, email addresses, phone numbers, Social Security numbers and/or driver's

license numbers ("personally identifiable information" or "PII").[1]

2. Beginning on September 7, 2023, hackers gained access to Defendant's network by impersonating an IT admin and gaining access credentials. The hackers then locked down Defendant's network preventing resort guests from using their electronic room cards, Wi-Fi, ATM kiosks, electronic gaming devices, and other resort services.

3. Two cybercriminal groups have taken credit for the attack against Defendant. First, a hacking group known as "The Scatter Spider "took credit, on or about September 11, 2021, for accessing and acquiring "six terabytes of data from the systems of multibillion-dollar casino operators MGM Resorts International[.]"[2] Second, a ransomware group known as ALPHV took credit, on or about September 14, 2023, for deploying a ransomware attack against Defendant and "download[ing] any and all exfiltrated materials", including "PII information contained in the exfiltrated data[]" involved in the cyberattack.[3] Though both groups took credit, they are likely operating as the same group, as are largely considered to be related.

4. Defendant owns and operates casino gaming brands with resorts throughout the United States, which include dining, live entertainment, accommodations, shopping, and gaming.

5. Upon information and belief, individuals, including Plaintiffs and Class Members, who were consumers of Defendant's entertainment services or sought to join the MGM Rewards

---

[1] Bill Toulas, *MGM Resorts Ransomware Attack Led to $100 Million Loss, Data Theft*, (Oct. 6, 2023), https://www.bleepingcomputer.com/news/security/mgm-resorts-ransomware-attack-led-to-100-million-loss-data-theft.

[2] Zeba Siddiqui, *Hackers Say They Stole 6 Terabytes of Data from Casino Giants MGM, Caesars* (Sept. 14, 2023), https://www.reuters.com/business/casino-giant-caesars-confirms-data-breach-2023-09-14.

[3] *Statement on MGM Resorts International: Setting the Record Straight* (Sept. 14, 2023), https://gist.githubusercontent.com/BushidoUK/20b81335c6729dc8e0b5997ca83fa35f/raw/a0697117e905f5094e7a5feae928806b2ba65b20/gistfile1.txt.

loyalty program are required to entrust Defendant with sensitive, non-public PII, without which Defendant could not perform its regular business activities, to obtain entertainment products and/or services from Defendant. Defendant retains this information for at least many years and even after the consumer relationship has ended.

6. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

7. Defendant failed to adequately protect Plaintiffs' and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect consumers' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

8. Defendant is a gaming and hospitality company that owns and operates 31 hotel and gaming destinations globally, including 12 hotels on the Las Vegas Strip. MGM is a publicly traded company and listed on the NASDAQ stock exchange with the ticket symbol "MGM".[4]

9. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices;

---

[4] MGM Resorts International, Securities and Exchange Commission Form 8-k, https://www.sec.gov/ix?doc=/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm.

and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

10. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party.

11. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

12. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

13. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen because of the Data Breach and who remain at risk due to Defendant's inadequate data

security practices.

II. PARTIES

14. Defendant is a Delaware corporation with its principal place of business in the State of Nevada at 3600 South Las Vegas Boulevard, Las Vegas, Nevada 89109.

15. Plaintiff Tonya Owens is a natural person and is a resident and citizen of the State of Mississippi, where she intends to remain.

16. Plaintiff Emily Kirwan is a natural person and is a resident and citizen of the State of Louisiana, where she intends to remain.

17. Plaintiff David Zussman is a natural person and is a resident and citizen of the State of Texas, where he intends to remain.

18. Plaintiff David Lackey is a natural person and is a resident and citizen of the Commonwealth of Virginia, where he intends to remain.

19. Plaintiff Michael Pircio is a natural person and is a resident and citizen of the State of Ohio, where he intends to remain.

20. Plaintiff David Terezo is a natural person and is a resident and citizen of the State of New York, where he intends to remain.

21. Plaintiff Ronald G. Rundell is a natural person and is a resident and citizen of the State of South Dakota, where he intends to remain.

22. Plaintiff Anita Johnson is a natural person and is a resident and citizen of the State of California, where she intends to remain.

23. Plaintiff Paul Zari is a natural person and is a resident and citizen of the Commonwealth of Virginia, where he intends to remain.

24. Plaintiff Michael Manson is a natural person and is a resident and citizen of the

State of Arizona, where he intends to remain.

25. Plaintiff Kyle Sloan is a natural person and is a resident and citizen of the State of Indiana, where he intends to remain.

26. Plaintiff Michelle Righetti is a natural person and is a resident and citizen of the State of California, where she intends to remain.

27. Plaintiff Edgar Mejia is a natural person and is a resident and citizen of the State of Nevada, where he intends to remain.

28. Plaintiff DuJun Johnson is a natural person and is a resident and citizen of the State of Nevada, where he intends to remain.

III. JURISDICTION AND VENUE

29. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds five million dollars, exclusive of interest and costs. Indeed, there are more than seventy-five million Class Members, and numerous plaintiffs who reside in diverse states.

30. This Court has jurisdiction over Defendant because it operates in this District.

31. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and Defendant has harmed Class Members residing in this District.

IV. GENERAL FACTUAL ALLEGATIONS

The Data Breach

32. On September 11, 2023, MGM posted a message on social media informing

consumers that MGM experienced a cybersecurity issue affecting some of its systems.[5]

33. Through its investigation, MGM determined that an unauthorized actor acquired, among other data, names, contact information (such as phone numbers, email addresses, and postal addresses), genders, dates of birth, and driver's license numbers of certain customers, and for some customers, social security numbers and/or passport numbers.[6]

34. According to news reports, the unauthorized actor is a hacking group known as Scattered Sider (or UNC3944) which is known for using social engineering to trick employees of the target company into granting them access to their network.[7]

35. On or around October 5, 2023, MGM filed a Form 8-K with the SEC to alert investors and shareholders that the Data Breach will have a negative impact on third quarter 2023 results.[8]

36. Also, around that time, MGM published an informational website regarding the Data Breach. While the website did not provide much detail about the scope and breadth of the Breach, it did state that at a minimum that phone numbers, email addresses, postal addresses, genders, dates of birth, and driver's license numbers of some of its customers were impacted, and that for a certain number of customers, social security numbers and/or passport numbers were also affected.[9] MGM stated that it is offering credit monitoring and identity theft protection services to

---

5 *See* Sean Morrison, *The Chaotic and Cinematic MGM Casino Hack, Explained*, VOX, https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware.

6 Notice of Data Breach, https://www.mgmresorts.com/en/notice-of-data-breach.html.

7 Carly Page & Zack Whittaker, *Hackers claim MGM cyberattack as outage drags into fourth day*, TECHCRUNCH (Sept. 14, 2023), https://techcrunch.com/2023/09/14/mgm-cyberattack-outage-scattered-spider.

8 SEC Form 8-K, *supra* n.4.

9 Notice of Data Breach, *supra* n.6.

customers impacted by the Data Breach.[10]

37. Plaintiffs' investigation has revealed that, in early summer 2023, hackers began intelligence gathering on MGM to identify employees and contractors that might have administrator level privileges to the MGM information systems. The hackers then began contacting the MGM help desk to impersonate those individuals and to convince the MGM help desk employees to reset the target's password, so that the hackers would have access to that MGM employee or contractor's account.

38. Ultimately, the hackers compromised multiple accounts, including administrator credentials.

39. Though not definitive, Plaintiffs' investigation revealed that data taken from MGM's systems has likely been circulated around the dark web.

40. Moreover, Plaintiffs' investigation revealed that the hackers likely exploited Defendant's help desk by convincing members of the IT help desk to reset passwords, allowing the hackers to gain initial access.

41. MGM is responsible for allowing the Data Breach to occur because it failed to implement and maintain reasonable safeguards, failed to comply with industry-standard data security practices, as well as federal and state laws and regulations governing data security, and failed to supervise, monitor, and oversee all third parties it hired who had access to Plaintiffs' and the Class Members' PII.

42. During the Data Breach, MGM failed to adequately monitor its information technology infrastructure. Had MGM done so, it would have prevented or mitigated the scope and

---

10 *Id.*

impact of the Data Breach.

43. Plaintiffs and Class Members provided their PII to MGM with the reasonable expectation and mutual understanding that MGM would comply with its obligations to keep such information confidential and secure from unauthorized access.

44. MGM's data security obligations were particularly important given the substantial increase in cyber and ransomware attacks and data breaches in the gaming and hospitality industries preceding the date of the Data Breach, as well as given the incredibly sensitive nature of PII that it retained in its servers.

45. By obtaining, collecting, and using Plaintiffs' and Class Members' PII, MGM assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

46. As a result of MGM's failure to protect sensitive PII it was entrusted with, Plaintiffs and Class Members are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Plaintiffs and Class Members have also lost the inherent value of their PII.

MGM Was on Notice of Data Breach Threats and the Inadequacy of Its Data Security

47. MGM's data security obligations were especially important given the substantial increase in cyberattacks and data breaches in recent years. In 2022, there were 1,802 reported data breaches, affecting approximately 422 million individuals.[11]

48. MGM should have been aware—and was aware—that it was at risk of an internal data breach that could expose the PII that it collected and maintained.

---

[11] *2022 Data Breach Report*, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf, at 2.

49. Despite this, MGM failed to take the necessary precautions required to safeguard Plaintiffs' and Class Members' PII from unauthorized access.

MGM Failed to Comply with Statutory and Regulatory Obligations

50. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[12]

51. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which establishes guidelines for fundamental data security principles and practices for business.[13] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating that someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[14]

52. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords for network access, use industry-tested methods for security, monitor

---

12 *Start with Security: A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205- startwithsecurity.pdf.

13 *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

14 *Id.*

for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[15]

53. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[16]

54. MGM also failed to comply with commonly accepted industry standards for data security. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

- Maintaining a secure firewall configuration;
- Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;
- Monitoring for suspicious or irregular traffic to servers;
- Monitoring for suspicious credentials used to access servers;
- Monitoring for suspicious or irregular activity by known users;
- Monitoring for suspicious or unknown users;
- Monitoring for suspicious or irregular server requests;
- Monitoring for server requests for PII;

---

15 *See Start with Security: A for Business*, FTC, *supra* n.12.

16 *See Privacy and Security Enforcement Press Releases*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

- Monitoring for server requests from VPNs; and
- Monitoring for server requests from Tor exit nodes.

55. MGM is also required by various states' laws and regulations to protect Plaintiffs' and Class Members' PII and to handle any breach of the same in accordance with applicable breach notification statutes.

56. In addition to its obligations under federal and state laws, MGM owed a duty to Plaintiffs and Class Members whose PII were entrusted to MGM to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. MGM owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its systems and networks adequately protected the PII of Plaintiffs and Class Members.

57. MGM owed a duty to Plaintiffs and Class Members whose PII was entrusted to MGM to design, maintain, and test its systems to ensure that the PII in MGM's possession was adequately secured and protected.

58. MGM owed a duty to Plaintiffs and Class Members whose PII was entrusted to MGM to create and implement reasonable data security practices and procedures to protect the PII in its possession.

59. MGM owed a duty to Plaintiffs and Class Members whose PII was entrusted to MGM to implement processes that would detect a breach on its data security systems in a timely manner.

60. MGM owed a duty to Plaintiffs and Class Members whose PII was entrusted to MGM to act upon data security warnings and alerts in a timely fashion.

61. MGM owed a duty to Plaintiffs and Class Members whose PII was entrusted to MGM to disclose if its systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust PII to MGM.

62. MGM owed a duty to Plaintiffs and Class Members whose PII was entrusted to MGM to disclose in a timely and accurate manner when data breaches occurred.

63. MGM owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequacy in its affirmative development of the systems to maintain PII and in its affirmative maintenance of those systems.

64. In this case, MGM was fully aware of its obligation to use reasonable measures to protect the PII of its customers. MGM also knew it was a target for hackers. But despite understanding the consequences of inadequate data security, MGM failed to comply with industry-standard data security requirements.

The Effect of the Data Breach on Impacted Consumers

65. The exponential cost to Plaintiffs and Class Members resulting from the Data Breach cannot be overstated. Criminals can use victims' PII to open new financial accounts, incur charges in credit, obtain governmental benefits and identifications, fabricate identities, and file fraudulent tax returns well before a person whose PII was stolen becomes aware of it.[17] Any one

---

[17] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737 (June 2007), https://www.gao.gov/new.items/d07737.pdf; *see also* Melanie Lockert, *How do hackers use your information for identity theft?*, CREDITKARMA (Oct. 1, 2021), https://www.creditkarma.com/id-theft/i/how-hackers-use-your-information; *see also* Ravi Sen, *Here's how much your personal information is worth to cybercriminals – and what they do with it*, PBS (May 14, 2021), https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it (last visited Oct. 17, 2023); *see also* Alison Grace

of these instances of identity theft can have devastating consequences for the victim, causing years of often irreversible damage to their credit scores, financial stability, and personal security.

66. Defendant was or should have been aware that it was collecting highly valuable data, which has increasingly been the target of data breaches in recent years.

67. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

68. The exposure of any PII can cause unexpected harms one would not ordinarily associate with the type of information stolen. Cybercriminals routinely aggregate Private Information from multiple illicit sources and use stolen information to gather even more information through social engineering, credential stuffing, and other methods. The resulting complete dossiers of PII are particularly prized among cybercriminals because they expose the target to every manner of identity theft and fraud.

69. Identity thieves can use PII such as that exposed in the Data Breach to: (a) apply for credit cards or loans (b) purchase prescription drugs or other medical services (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits or insurance benefits; (f) file a fraudulent tax return using the victim's information; (g) commit espionage; or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

Johansen, *4 Lasting Effects of Identity Theft*, LIFELOCK BY NORTON (Feb. 4, 2021), https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-ofidentity-theft.

Diminution of Value of PII

70. PII is valuable property.[18] Its value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates, beyond doubt, that PII has considerable market value.

71. The PII stolen in the Data Breach is significantly more valuable than the loss of credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements.

72. This type of data commands a much higher price on the dark web. As Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information … [is] worth more than 10x on the black market."[19]

73. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[20]

74. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[21] Indeed, a Social Security number, date of

---

18 *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737 (June 2007), https://www.gao.gov/new.items/d07737.pdf, at 2.

19 Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

20 *See, e.g.,* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

21 David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, L.A.

birth, and full name can sell for $60 to $80 on the digital black market.[22]

75. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

76. The fraudulent activity resulting from the Data Breach may not come to light for years.

77. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

78. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to millions of individuals' detailed PII and thus the significant number of individuals who would be harmed by the exposure of the unencrypted data.

79. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[22] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, PCMAG (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

80. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm.

81. Class Members have spent, and will spend, time on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon seeing news reports and monitoring their credit reports and financial accounts for suspicious activity, as MGM advised in its online notice.[23]

82. These mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches, in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[24]

83. Plaintiffs' mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on

---

23 *See* Notice of Data Breach, *supra* n.6.

24 *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, *supra* n.18.

their credit, and correcting their credit reports.[25]

84. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

85. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to millions of individuals' detailed PII and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

86. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Impact of Identity Theft Can Have Ripple Effects

87. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of a Social Security number, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.

88. And, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they

---

[25] *See Identity Theft.gov*, FTC, https://www.identitytheft.gov/Steps.

experienced affected their ability to get credit cards and obtain loans such as student loans or mortgages.[26] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

89. It is no wonder then that identity theft exacts a severe emotional toll on its victims.

90. The 2017 Identity Theft Resource Center survey[27] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported that a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.

91. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate and/or lack of focus;
- 28.7% reported that they were unable to go to work because of physical symptoms;

---

[26] Identity Theft Res. Ctr., *Identity Theft: The Aftermath 2017*, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf.

[27] *Id.*

- 23.1% reported new physical illnesses, including aches and pains, heart palpitations, sweating, and/or stomach issues;
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[28]

92. There may also be a significant time lag between when PII is stolen and when it is actually misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[29]

93. As the result of the Data Breach, Plaintiffs and Class Members have suffered and/or will suffer or continue to suffer economic loss, a substantial risk of future identity theft, and other actual harm for which they are entitled to damages, including, but not limited to, the following:

- Losing the inherent value of their PII;
- Losing the value of Defendant's implicit promises of adequate data security;
- Identity theft and fraud resulting from the theft of their PII;
- Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;
- Costs associated with purchasing credit monitoring and identity theft protection services;

---

28 *Id.*

29 *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, *supra* n.18.

- Unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- Lowered credit scores resulting from credit inquiries following fraudulent activities;
- Costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and
- The continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being in the possession of one or many unauthorized third parties.

94. Additionally, Plaintiffs and Class Members place significant value in data security.

95. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, companies like Defendant would have no reason to tout their data security efforts to their actual and potential customers.

96. Consequently, had consumers known the truth about Defendant's data security

practices—that Defendant would not adequately protect and store their data—they would not have entrusted their PII to Defendant, purchased insurance that included Defendant's services, or paid as much for such services or benefits.

97. As such, Plaintiffs and Class Members did not receive the benefit of their bargain with Defendant because they entrusted their PII and purchased accommodations, dining, gaming and other goods and services with the reasonable expectation that Defendant would adequately protect and store their data, which it did not.

V. PLAINTIFFS' EXPERIENCES

Plaintiff Tonya Owens

98. Plaintiff Tonya Owens ("Plaintiff Owens") is a current MGM Rewards member.

99. In order to obtain an MGM Rewards membership, Plaintiff Owens was required to provide her PII to Defendant, including her name, date of birth, contact information, and Social Security number.

100. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Owens's PII in its system.

101. Plaintiff Owens is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

102. Plaintiff Owens would not have entrusted her PII to Defendant had she known of Defendant's lax data security policies.

103. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff Owens made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with

the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

104. Plaintiff Owens suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

105. The Data Breach has caused Plaintiff Owens to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

106. As a result of the Data Breach, Plaintiff Owens anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

107. As a result of the Data Breach, Plaintiff Owens is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

108. Plaintiff Owens has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Emily Kirwan

109. Plaintiff Emily Kirwan ("Plaintiff Kirwan") is a current MGM Rewards member.

110. In order to obtain an MGM Rewards membership, Plaintiff Kirwan was required to provide her PII to Defendant, including her name, date of birth, contact information, and Social Security number.

111. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Kirwan's PII in its system.

112. Plaintiff Kirwan is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

113. Plaintiff Kirwan would not have entrusted her PII to Defendant had she known of Defendant's lax data security policies.

114. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff Kirwan made reasonable efforts to mitigate the impact of the Data Breach, including changing her debit card pin number and monitoring her financial accounts for fraudulent activity. Plaintiff Kirwan has spent significant time dealing with the Data Breach–valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

115. Plaintiff Kirwan suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data

Breach; and (vii) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

116. The Data Breach has caused Plaintiff Kirwan to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

117. As a result of the Data Breach, Plaintiff Kirwan anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

118. As a result of the Data Breach, Plaintiff Kirwan is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

119. Plaintiff Kirwan has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff David Zussman

120. Plaintiff David Zussman ("Plaintiff Zussman") is a current MGM Rewards member.

121. In order to obtain an MGM Rewards membership, Plaintiff Zussman was required to provide his PII to Defendant, including his name, date of birth, contact information, and Social Security number.

122. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Zussman's PII in its system.

123. Plaintiff Zussman is very careful about sharing his sensitive PII. Plaintiff Zussman stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

124. Plaintiff Zussman would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

125. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff Zussman made reasonable efforts to mitigate the impact of the Data Breach, including monitoring his financial accounts for fraudulent activity. Plaintiff Zussman has spent significant time dealing with the Data Breach—valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

126. Plaintiff Zussman suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

127. The Data Breach has caused Plaintiff Zussman to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

128. As a result of the Data Breach, Plaintiff Zussman anticipates spending considerable

time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

129. As a result of the Data Breach, Plaintiff Zussman is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

130. Plaintiff Zussman has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff David Lackey

131. Plaintiff David Lackey ("Plaintiff Lackey") is a current MGM Rewards member. He joined Defendant's rewards program over twenty years ago, and Plaintiff Lackey has, on several occasions, visited MGM National Harbor in Oxon Hill, Maryland and also visits MGM properties in Las Vegas, Nevada.

132. In order to obtain an MGM Rewards membership, Plaintiff Lackey was required to provide his PII to Defendant, including his name, date of birth, contact information, and Social Security number.

133. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Lackey's PII in its system.

134. Plaintiff Lackey is very careful about sharing his sensitive PII. Plaintiff Lackey stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

135. Plaintiff Lackey would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

136. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff

Lackey made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Lackey has spent significant time dealing with the Data Breach—valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

137. Further, as a result of the Data Breach, Plaintiff Lackey received increased text phishing attempts from multiples sources in the weeks following the Data Breach.

138. Plaintiff Lackey suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

139. The Data Breach has caused Plaintiff Lackey to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

140. As a result of the Data Breach, Plaintiff Lackey anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

141. As a result of the Data Breach, Plaintiff Lackey is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

142. Plaintiff Lackey has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Michael Pircio

143. Plaintiff Michael Pircio ("Plaintiff Pircio") is a current MGM Rewards member, who last stayed at Defendant's resorts in early September 2023.

144. In order to obtain an MGM Rewards membership, Plaintiff Pircio was required to provide his PII to Defendant, including his name, date of birth, contact information, and Social Security number.

145. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Pircio's PII in its system.

146. Plaintiff Pircio is very careful about sharing his sensitive PII. Plaintiff Pircio stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

147. Plaintiff Pircio would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

148. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff Pircio made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Pircio has spent significant time dealing with the Data Breach, including time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring his accounts with heightened scrutiny and time spent seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This is valuable time he otherwise would have spent on other activities, including but not limited

to work and/or recreation. This time has been lost forever and cannot be recaptured.

149. Plaintiff Pircio suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

150. The Data Breach has caused Plaintiff Pircio to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

151. As a result of the Data Breach, Plaintiff Pircio anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

152. As a result of the Data Breach, Plaintiff Pircio is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

153. Plaintiff Pircio has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff David Terezo

154. Plaintiff David Terezo ("Plaintiff Terezo") is a current MGM Rewards member.

155. In order to obtain an MGM Rewards membership, Plaintiff Terezo was required to provide his PII to Defendant, including his name, date of birth, contact information, and Social Security number.

156. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Terezo's PII in its system.

157. Plaintiff Terezo is very careful about sharing his sensitive PII. Plaintiff Terezo stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

158. Plaintiff Terezo would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

159. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff Terezo made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Terezo has spent significant time dealing with the Data Breach, including changing his debit card pin number and monitoring his financial accounts for fraudulent activity—valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

160. Plaintiff Terezo suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains

backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

161. The Data Breach has caused Plaintiff Terezo to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

162. As a result of the Data Breach, Plaintiff Terezo anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

163. As a result of the Data Breach, Plaintiff Terezo is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

164. Plaintiff Terezo has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Ronald G. Rundell

165. Plaintiff Ronald G. Rundell ("Plaintiff Rundell") is a current MGM Rewards member since before 2018.

166. In order to obtain an MGM Rewards membership, Plaintiff Rundell was required to provide his PII to Defendant, including his name, date of birth, contact information, and Social Security number.

167. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Rundell's PII in its system.

168. Plaintiff Rundell is very careful about sharing his sensitive PII. Plaintiff Rundell stores any documents containing his PII in a safe and secure location. He has never knowingly

transmitted unencrypted sensitive PII over the internet or any other unsecured source.

169. Plaintiff Rundell would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

170. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff Rundell made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Rundell has spent significant time dealing with the Data Breach, including reviewing account statements and monitoring credit reports—valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

171. Plaintiff Rundell suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

172. The Data Breach has caused Plaintiff Rundell to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

173. As a result of the Data Breach, Plaintiff Rundell anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data

Breach.

174. As a result of the Data Breach Plaintiff Rundell is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

175. Plaintiff Rundell has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Paul Zari

176. Plaintiff Paul Zari ("Plaintiff Zari") is a current MGM Rewards member.

177. In order to obtain an MGM Rewards membership, Plaintiff Zari was required to provide his PII to Defendant, including his name, date of birth, contact information, and Social Security number.

178. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Zari's PII in its system.

179. Plaintiff Zari is very careful about sharing his sensitive PII. Plaintiff Zari stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

180. Plaintiff Zari would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

181. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff Zari made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Zari has spent significant time dealing with the Data Breach—valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

182. Plaintiff Zari suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

183. The Data Breach has caused Plaintiff Zari to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

184. As a result of the Data Breach, Plaintiff Zari anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

185. As a result of the Data Breach, Plaintiff Zari is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

186. Plaintiff Zari has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Michael Manson

187. Plaintiff Michael Manson ("Plaintiff Manson") is a current MGM Rewards member.

188. In order to obtain an MGM Rewards membership, Plaintiff Manson was required

to provide his PII to Defendant, including his name, date of birth, contact information, and Social Security number.

189. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Manson's PII in its system.

190. Plaintiff Manson is very careful about sharing his sensitive PII. Plaintiff Manson stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

191. Plaintiff Manson would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

192. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff Manson made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Manson has spent significant time dealing with the Data Breach—valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

193. Plaintiff Manson suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

194. The Data Breach has caused Plaintiff Manson to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

195. As a result of the Data Breach, Plaintiff Manson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

196. As a result of the Data Breach, Plaintiff Manson is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

197. Plaintiff Manson has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Kyle Sloan

198. Plaintiff Kyle Sloan ("Plaintiff Sloan") is a current MGM Rewards member since December 2021.

199. In order to obtain an MGM Rewards membership, Plaintiff Sloan was required to provide his PII to Defendant, including his name, date of birth, contact information, and Social Security number.

200. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Sloan's PII in its system.

201. Plaintiff Sloan is very careful about sharing his sensitive PII. Plaintiff Sloan stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

202. Plaintiff Sloan would not have entrusted his PII to Defendant had he known of

Defendant's lax data security policies.

203. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff Sloan made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Sloan has spent significant time dealing with the Data Breach, including self-monitoring accounts and credit reports to ensure no fraudulent activity has occurred, such as checking his bank accounts and credit cards every day to look for unauthorized or suspicious activity, and checking his Experian ID theft monitoring account routinely since the Data Breach. This is valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

204. Plaintiff Sloan suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

205. Further, Plaintiff Sloan has noticed an increase in spam calls since the Data Breach.

206. The Data Breach has caused Plaintiff Sloan to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

207. As a result of the Data Breach, Plaintiff Sloan anticipates spending considerable

time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

208. As a result of the Data Breach, Plaintiff Sloan is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

209. Plaintiff Sloan has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Michelle Righetti

210. Plaintiff Michelle Righetti ("Plaintiff Righetti") is a current MGM customer.

211. In order to receive Defendant's services, Plaintiff Righetti was required to provide her PII to Defendant, including her name, date of birth, contact information, and Social Security number.

212. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Righetti's PII in its system.

213. Plaintiff Righetti is very careful about sharing her sensitive PII. Plaintiff Righetti stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

214. Plaintiff Righetti would not have entrusted her PII to Defendant had she known of Defendant's lax data security policies.

215. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff Righetti made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Righetti has spent significant time dealing with the Data Breach—valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost

forever and cannot be recaptured.

216. Plaintiff Righetti suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

217. The Data Breach has caused Plaintiff Righetti to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

218. As a result of the Data Breach, Plaintiff Righetti anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

219. As a result of the Data Breach, Plaintiff Righetti is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

220. Plaintiff Righetti has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Edgar Mejia

221. Plaintiff Edgar Mejia ("Plaintiff Mejia") is a current MGM customer.

222. In order to receive Defendant's services, Plaintiff Mejia was required to provide his PII to Defendant, including his name, date of birth, contact information, and Social Security number.

223. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Mejia's PII in its system.

224. Plaintiff Mejia is very careful about sharing his sensitive PII. Plaintiff Mejia stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

225. Plaintiff Mejia would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

226. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff Mejia made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Mejia has spent significant time dealing with the Data Breach—this is valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

227. Plaintiff Mejia suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as

Defendant fails to undertake appropriate and adequate measures to protect the PII.

228. The Data Breach has caused Plaintiff Mejia to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

229. As a result of the Data Breach, Plaintiff Mejia anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

230. As a result of the Data Breach, Plaintiff Mejia is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

231. Plaintiff Mejia has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff DuJun Johnson

232. Plaintiff DuJun Johnson ("Plaintiff D. Johnson") is a current MGM customer.

233. In order to receive Defendant's services, Plaintiff D. Johnson was required to provide his PII to Defendant, including his name, date of birth, contact information, and Social Security number.

234. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff D. Johnson's PII in its system.

235. Plaintiff D. Johnson is very careful about sharing his sensitive PII. Plaintiff D. Johnson stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

236. Plaintiff D. Johnson would not have entrusted his PII to Defendant had he known

of Defendant's lax data security policies.

237. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff D. Johnson made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff D. Johnson has spent significant time dealing with the Data Breach—this is valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

238. Plaintiff D. Johnson suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

239. The Data Breach has caused Plaintiff D. Johnson to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

240. As a result of the Data Breach, Plaintiff D. Johnson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

241. As a result of the Data Breach, Plaintiff D. Johnson is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

242. Plaintiff D. Johnson has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

VI. CLASS ACTION ALLEGATIONS

243. Plaintiffs bring this action on behalf of himself and the members of the proposed Class, which consists of:

> **Nationwide Class:** All persons in the United States whose Private Information was accessed during the Data Breach.
>
> **California Subclass:** All persons in California whose Private Information was accessed during the Data Breach.

244. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

245. Plaintiffs reserve the right to amend the above definition or to propose subclasses before the Court determines whether certification is appropriate.

246. **Numerosity**: The proposed Class is so numerous that joinder of all members is impracticable. Based on informal discovery, the Class is believed to be approximately seventy-five million individuals.

247. **Typicality**: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Defendant.

248. **Adequacy**: Plaintiffs is an adequate representative of the Class because Plaintiffs' interests do not conflict with the interests of the Class; Plaintiffs has retained competent counsel who are experienced in prosecuting complex class action and data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

249. **Superiority**: A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the claims of all members of the Class is economically unfeasible and procedurally impracticable. The injury suffered by each individual member of the Class is relatively small in comparison to the burden and expense of individual prosecution of litigation. It would be very difficult for members of the Class to effectively redress Defendant's wrongdoing. Further, individualized litigation presents a potential for inconsistent or contradictory judgments.

250. **Commonality and Predominance**: There are numerous questions of law and fact common to the Class which predominate over any questions affecting only individual members of the Class.

251. Among the questions of law and fact common to the Class are:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's PII;

c. Whether Defendant negligently hired and/or failed to supervise the third-party vendor it hired and gave access to Plaintiffs' and the Class's PII;

d. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their PII, and whether it breached this duty;

e. Whether Defendant breached its duties to Plaintiffs and the Class as a result of the

Data Breach;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach;

g. Whether Defendant was negligent in permitting the third-party access to Plaintiffs' and the Class's PII;

h. Whether Defendant was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach;

i. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

j. Whether Defendant continues to breach duties to Plaintiffs and the Class;

k. Whether Plaintiffs and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

l. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief; and

m. Whether Defendant's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to punitive damages.

VII. COUNTS

FIRST CAUSE OF ACTION
NEGLIGENCE
(By Plaintiffs and on Behalf of the Class)

252. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

253. Defendant owed a duty of care to Plaintiffs and Class Members to use reasonable

means to secure and safeguard the entrusted PII, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems, as alleged herein. These common law duties existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices in Defendant's affirmative development and maintenance of its data security systems and its hiring of third-party providers entrusted with accessing, storing, safeguarding, handling, collecting, and/or protecting Plaintiffs' and Class Members' PII. In fact, not only was it foreseeable that Defendant and Class Members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendant also knew that it was more likely than not that Plaintiffs and other Class Members would be harmed by such exposure and theft of their PII.

254. Defendant's duties to use reasonable security measures also arose because of a special relationship with Plaintiffs and Class Members because of being entrusted with their PII, which provided an independent duty of care. Plaintiffs' and Class Members' willingness to entrust Defendant with their PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, Defendant could protect its network and systems, and the PII it stored on them, from unauthorized access.

255. Defendant's duties to use reasonable data security measures also arose under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII. Various FTC publications and data security breach orders further form the basis of Defendant's duties.

256. Defendant breached the aforementioned duties when it failed to use security

practices that would protect the PII provided to it by Plaintiffs and Class Members, thus resulting in unauthorized exposure and access to Plaintiffs' and Class Members' PII.

257. Defendant further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiffs' and Class Members' PII within its possession, custody, and control.

258. As a direct and proximate cause of Defendant's failure to use appropriate security practices and failure to select a third-party provider with adequate data security measures, Plaintiffs' and Class Members' PII was exposed, disseminated, and made available to unauthorized third parties.

259. Defendant admitted that Plaintiffs' and Class Members' PII was wrongfully disclosed as a result of the Data Breach.

260. The Data Breach caused direct and substantial damages to Plaintiffs and Class Members, as well as the likelihood of future and imminent harm through the dissemination of their PII and the greatly enhanced risk of credit fraud and identity theft.

261. By engaging in the foregoing acts and omissions, Defendant committed the common law tort of negligence. For all the reasons stated above, Defendant's conduct was negligent and departed from reasonable standards of care including by, but not limited to failing to adequately limit access to and protect the PII; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiffs' and Class Members' PII.

262. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

263. Neither Plaintiffs nor Class Members contributed to the Data Breach or subsequent misuse of their PII as described in this Complaint.

264. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Defendant, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(By Plaintiffs and on Behalf of the Class)

265. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

266. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

267. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing

to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach.

268. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

269. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

270. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of Defendant's failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

271. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Defendant, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their

bargains and overcharges for services; and other economic and non-economic harm.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(By Plaintiffs and on Behalf of the Class)

272. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

273. Plaintiffs and Class Members entered into an implied contract with MGM when they obtained products or services from MGM, joined the loyalty program, or otherwise provided PII to MGM.

274. As part of these transactions, MGM agreed to safeguard and protect the PII of Plaintiffs and Class Members and to timely and accurately notify them if their PII was breached or compromised.

275. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that MGM's data security practices and policies were reasonable and consistent with legal requirements and industry standards. Plaintiffs and Class Members believed that MGM would use part of the monies paid to MGM under the implied contracts or the monies obtained from the benefits derived from the PII they provided to fund proper and reasonable data security practices.

276. Plaintiffs and Class Members would not have provided and entrusted their PII to MGM or would have paid less for MGM products or services in the absence of the implied contract or implied terms between them and MGM. The safeguarding of the PII of Plaintiffs and Class Members was critical to realize the intent of the parties.

277. Plaintiffs and Class Members fully performed their obligations under the implied contracts with MGM.

278. MGM breached its implied contracts with Plaintiffs and Class Members to protect their PII when it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties.

279. As a direct and proximate result of MGM's breach of implied contract, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of MGM's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(In the alternative)
(By Plaintiffs and on Behalf of the Class)

280. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

281. This claim is pleaded in the alternative to the Breach of Implied contract claim set forth in the Third Cause of Action.

282. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by Defendant and that was ultimately stolen in the Data Breach.

283. Defendant benefitted from the conferral upon it of the PII pertaining to Plaintiffs and Class Members and by its ability to retain, use, sell, and profit from that information. MGM understood that it was in fact so benefitted.

284. MGM also understood and appreciated that the PII pertaining to Plaintiffs and Class Members was private and confidential and its value depended upon MGM maintaining the privacy and confidentiality of that PII.

285. But for MGM's willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and Class Members would not have provided their PII to MGM or would not have permitted MGM to gather additional PII.

286. Plaintiffs' and Class Members' PII has an independent value to MGM.

287. MGM admits that it uses the PII it collects for, among other things, "recording and accessing gaming-related activity," "customizing [customers] experience while visiting, using and/or accessing MGM Online Services and/or MGM Resorts," "protecting and defending MGM Resorts International and its affiliates against legal actions or claims," "satisfying contractual obligations," "assess[ing] and improv[ing] [its] products and services," and "conducting internal research, analytics, and statistical or demographic analysis."[30]

288. Because of its use of Plaintiffs' and Class Members' PII, MGM sold more services and products than it otherwise would have. MGM was unjustly enriched by profiting from the

---

[30] Privacy Policy, MGM (July 10, 2023), https://www.mgmresorts.com/en/privacy-policy.html.

additional services and products it was able to market, sell, and create through the use of Plaintiffs' and Class Members' PII to the detriment of Plaintiffs and Class Members.

289. MGM also benefitted through its unjust conduct by retaining money paid by Plaintiffs and Class Members that it should have used to provide proper data security to protect Plaintiffs' and Class Members' PII.

290. It is inequitable for MGM to retain these benefits.

291. As a result of MGM'S wrongful conduct as alleged in this Complaint (including among other things its failure to employ proper data security measures, its continued maintenance and use of the PII belonging to Plaintiffs and Class Members without having proper data security measures, and its other conduct facilitating the theft of that PII), MGM has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

292. MGM'S unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Members' sensitive PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

293. It is inequitable, unfair, and unjust for MGM to retain these wrongfully obtained benefits. MGM'S retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

294. The benefit conferred upon, received, and enjoyed by MGM was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for MGM to retain the benefit.

295. MGM'S defective security and its unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to

mitigate and monitor the use of their PII and has caused the Plaintiffs and Class Members other damages as described herein.

296. Plaintiffs have no adequate remedy at law.

297. MGM is therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on MGM as a result of its wrongful conduct, including specifically: the value to MGM of the PII that was stolen in the Data Breach; the profits MGM received and is receiving from the use of that information; the amounts that MGM overcharged Plaintiffs and Class Members for use of MGM's products and services; and the amounts that MGM should have spent to provide proper data security to protect Plaintiffs' and Class Members' PII.

FIFTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(By Plaintiffs and on Behalf of the Class)

298. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

299. Plaintiffs and Class Members maintained a confidential relationship with MGM whereby MGM undertook a duty not to disclose to unauthorized parties the PII that Plaintiffs and Class Members provide to MGM. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

300. MGM knew Plaintiffs' and Class Members' PII was disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII it collected, stored, and maintained.

301. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs' and Class Members' PII in violation of this understanding. The unauthorized disclosure occurred

because MGM failed to implement and maintain reasonable safeguards to protect the PII in its possession and failed to comply with industry-standard data security practices.

302. Plaintiffs and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

303. But for MGM'S actions and inactions in violation of the parties' understanding of confidence, the PII of Plaintiffs and Class Members would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. MGM'S actions and inaction were the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.

304. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of MGM'S unauthorized disclosure of Plaintiffs' and Class Members' PII. MGM knew its computer systems and technologies for accepting, securing, and storing Plaintiffs' and Class Members' PII had serious security vulnerabilities because MGM failed to observe even basic information security practices or correct known security vulnerabilities.

305. As a direct and proximate result of MGM'S breach of confidence, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related

activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of MGM'S Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

306. By collecting and storing this PII and using it for commercial gain, MGM has a duty of care to use reasonable means to secure and safeguard this PII to prevent disclosure and guard against theft of the PII.

SIXTH CAUSE OF ACTION
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL")
UNLAWFUL BUSINESS PRACTICE
(Cal Bus. & Prof. Code § 17200, *et seq*.)
(By Plaintiffs Anita Johnson and Michelle Righetti, on Behalf of the California Subclass)

307. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

308. Plaintiffs Johnson and Righetti bring this Count on their own behalf and on behalf of the California Class (the "Class" for the purposes of this Count).

309. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

310. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*. (the "CCPA"), and other state data security laws.

311. Defendant stored the PII of Plaintiffs and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate

security measures that complied with applicable regulations and that would have kept Plaintiffs' and the Class's PII secure so as to prevent the loss or misuse of that PII.

312. Defendant failed to disclose to Plaintiffs and the Class that their PII was not secure. However, Plaintiffs and the Class were entitled to assume, and did assume that Defendant had secured their PII. At no time were Plaintiffs and the Class on notice that their PII was not secure, which Defendant had a duty to disclose.

313. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' and the Class's nonencrypted and nonredacted PII.

314. Had Defendant complied with these requirements, Plaintiffs and the Class would not have suffered the damages related to the data breach.

315. Defendant's conduct was unlawful, in that it violated the CCPA.

316. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the Federal Trade Commission Act.

317. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

318. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting PII.

319. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all

individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

320. Instead, Defendant made the PII of Plaintiffs and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiffs and the Class to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

321. As a result of those unlawful and unfair business practices, Plaintiffs and the Class suffered an injury-in-fact and have lost money or property.

322. The injuries to Plaintiffs and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

323. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

324. Therefore, Plaintiffs and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

SEVENTH CAUSE OF ACTION
VIOLATION OF THE CALIFORNIA CONSUMER RECORDS ACT
Cal. Civ. Code § 1798.80, *et seq*.
(By Plaintiffs Anita Johnson and Michelle Righetti, on Behalf of the California Subclass)

325. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

326. Plaintiffs Johnson and Righetti bring this Count on their own behalf and on behalf of the California Class (the "Class" for the purposes of this Count).

327. Under California law, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82.) The disclosure must "be made in the most expedient time possible and without unreasonable delay" (Id.), but "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82, subdiv. b.)

328. The Data Breach constitutes a "breach of the security system" of Defendant.

329. An unauthorized person acquired the personal, unencrypted information of Plaintiffs and the Class.

330. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiffs and the Class, but waited approximately fourteen months to notify them. Fourteen months was an unreasonable delay under the circumstances.

331. Defendant's unreasonable delay prevented Plaintiffs and the Class from taking appropriate measures from protecting themselves against harm.

332. Because Plaintiffs and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

333. Plaintiffs and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

EIGHTH CAUSE OF ACTION
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code § 1798.150
(By Plaintiffs Anita Johnson, and Michelle Righetti, and on Behalf of the California Subclass)

334. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

335. Plaintiffs Johnson and Righetti bring this Count on their behalf and on behalf of the California Class (the "Class" for the purposes of this Count).

336. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiffs and the Class. As a direct and proximate result, Plaintiffs', and the Class's nonencrypted and nonredacted PII was subject to unauthorized access and exfiltration, theft, or disclosure.

337. Defendant is a business organized for the profit and financial benefit of its owners according to California Civil Code § 1798.140, that collects the personal information of its customers, and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

338. Plaintiffs and Class Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII,

including Plaintiffs' and Class Members' PII. Plaintiffs and Class Members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

339. Pursuant to California Civil Code § 1798.150(b), Plaintiffs mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and Plaintiffs believes such cure is not possible under these facts and circumstances—then Plaintiffs intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

340. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

341. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

NINTH CAUSE OF ACTION
VIOLATION OF THE NEVADA CONSUMER FRAUD ACT
Nev. Rev. Stat. § 41.600
(By Plaintiffs and on Behalf of the Class)

342. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporate them at this point by reference as though set forth in full.

343. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600, states:

> 1. An action may be brought by any person who is a victim of consumer fraud.
>
> 2. As used in this section, "consumer fraud" means: . . . (e) A deceptive trade practice as defined in NRS 598.0915 to 598.0925, inclusive.

344. In turn, Nev. Rev. Stat. § 598.0923(2) (a section of the Nevada Deceptive Trade Practices Act) states: "A person engages in a 'deceptive trade practice' when in the course of his

or her business or occupation he or she knowingly: . . . 2) Fails to disclose a material fact in connection with the sale or lease of goods or services." MGM violated this provision because it failed to disclose the material fact that its data security practices were deficient and that its cloud server security settings were not adequate to protect consumers' PII. MGM knew or should have known that its data security practices were deficient. This is true because, among other things, MGM was aware that the hotel industry was a frequent target of sophisticated cyberattacks. MGM knew or should have known that its cloud server data security practices were insufficient to guard against those attacks. MGM had knowledge of the facts that constituted the omission. MGM could and should have made a proper disclosure when accepting hotel reservations, during the check-in process, in the registration for its MGM Rewards loyalty program, in its Privacy Policy, or by any other means reasonably calculated to inform consumers of its inadequate data security.

345. Also, Nev. Rev. Stat. § 598.0923(3) states: "A person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly: . . . 3) Violates a state or federal statute or regulation relating to the sale or lease of . . . services." MGM violated this provision for several reasons, each of which is an independent predicate act for purposes of violating § 598.0923(3).

346. *First*, MGM breached a Nevada statue requiring reasonable data security. Specifically, Nev. Rev. Stat. § 603A.210(1) states: "A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain *reasonable security measures* to protect those records from unauthorized access, acquisition, . . . use, modification or disclosure." (Emphasis added.) MGM is a data collector as defined under the statute at Nev. Rev. Stat. § 603A.030. MGM failed to implement and maintain reasonable security measures, evidenced by the fact that hackers accessed its cloud server and stole consumers' PII.

MGM's violation of this statute was done knowingly for purposes of Nev. Rev. Stat. § 598.0923(3). MGM knew or should have known that its data security practices were deficient. This is true because, among other things, MGM was aware that the hotel industry was a frequent target of sophisticated cyberattacks. MGM knew or should have known that its cloud server data security practices were insufficient to guard against those attacks. MGM had knowledge of the facts that constituted the violation.

347. *Second*, MGM breached other state statues as alleged herein. MGM also violated Nev. Rev. Stat. § 598.0923(2) as alleged in this Count. MGM knew or should have known that it violated these statutes. MGM's violation of each of these statutes serves as a separate predicate act for purposes of violating Nev. Rev. Stat. § 598.0923(3).

348. *Third*, MGM violated the FTC Act, 15 U.S.C. § 45, as alleged above. MGM knew or should have known that its data security practices were deficient, violated the FTC Act, and that it failed to adhere to the FTC's data security guidance for businesses. This is true because, among other things, MGM was aware that the hotel industry was a frequent target of sophisticated cyberattacks. MGM knew or should have known that its cloud server data security practices were insufficient to guard against those attacks. MGM had knowledge of the facts that constituted the violation. MGM's violation of the FTC Act serves as a predicate act for violating Nev. Rev. Stat.§ 598.0923(3).

349. MGM engaged in deceptive or unfair practices by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Class Members.

350. Plaintiffs and Class Members were denied a benefit conferred on them by the Nevada legislature.

351. Nev. Rev. Stat. § 41.600(3) states that if the Plaintiffs prevail, the court "shall

award: (a) Any damages that the claimant has sustained; (b) Any equitable relief that the court deems appropriate; and (c) the claimant's costs in the action and reasonable attorney's fees."

352. As a direct and proximate result of the foregoing, Plaintiffs and Class Members suffered all forms of damages alleged herein. Plaintiffs' harms constitute compensable damages under Nev. Rev. Stat. § 41.600(3).

353. Plaintiffs and Class Members are also entitled to all forms of injunctive relief sought herein.

354. Plaintiffs and Class Members are also entitled to an award of their attorney's fees and costs.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs, Tonya Owens, Emily Kirwan, David Zussman, David Lackey, Michael Pircio, David Terezo, Ronald G. Rundell, Anita Johnson, Paul Zari, Michael Manson, Kyle Sloan, Michelle Righetti, Edgar Mejia, and DuJun Johnson, individually and on behalf of the Class, request that the Court:

A. Certify this case as a class action on behalf of the Class defined above pursuant to Rule 23(b)(2), appoint Plaintiffs as the Class Representatives;

B. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

C. Award injunctive relief requiring Defendant to provide an accounting identifying all members of the class and Class;

D. Enter a declaratory judgment that Defendant committed negligence and negligence *per se* and that Defendant breached its implied contract with Plaintiffs and the Class;

E. Award injunctive relief enjoining Defendant from engaging in future negligence, negligence *per se*, and breaches of contract;

F. Award injunctive relief requiring Defendant to provide notice to all members of the class that its data breach constituted negligence, negligence per se, and a breach of its implied contracts with the Class, and that if they were harmed that they can bring individual actions for common law relief for damages under negligence, negligence per se, and breach of implied contract claims; and

G. Award such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

Dated: January 30, 2025

Respectfully submitted,

/s/ Nathan R. Ring
Nathan R. Ring
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102
(725) 235-9750
lasvegas@stranchlaw.com

Liaison Counsel

J. Gerard Stranch, IV
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
(615) 254-8801
gstranch@stranchlaw.com

Lynn A. Toops
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
(317) 636-6481
ltoops@cohenandmalad.com

James J. Pizzirusso
HAUSFELD LLP

888 16th Street, Suite 300
Washington, DC 20006
(202) 540-7200
jpizzirusso@hausfeld.com

Interim Lead Counsel

Mariya Weekes
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
201 Sevilla Avenue, 2nd Floor
Coral Gables, FL 33134
(786) 879-8200
mweekes@milberg.com

Jeff Ostrow
KOPELOWITZ OSTROW, P.A.
One West Las Olas Boulevard, Suite 500
Fort Lauderdale, FL 33301
(954) 525-4100
ostrow@kolawyers.com

Marc Dann
DANNLAW
15000 Madison Avenue
Lakewood, OH 44107
(216) 373-0539
mdann@dannlaw.com

Rachele R. Byrd
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
(619) 239-4599
byrd@whafh.com

Tom Loeser
COTCHETT, PITRE & MCCARTHY
840 Malcolm Road
Burlingame, CA 94010
650-697-6000
tloeser@cpmlegal.com

Maureen M. Brady
MCSHANE & BRADY, LCC
1656 Washington Street, Suite 120
Kansas City, MO 64108
(816) 888-8010
mbrady@mcshanebradylaw.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN
510 Walnut Street, Suite 500

Philadelphia, PA 19106
(215) 592-4663
cschaffer@lfsblaw.com

James E. Cecchi
CARELLA BYRNE CECCHI OLSTEIN BRODY & AGNELLO
5 Becker Farm Road, 2nd Floor
Roseland, NJ 07068
973-994-1700
jcecchi@carellabyrne.com

Plaintiffs' Steering Committee

Counsel for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

It is hereby certified that a true and accurate copy of the foregoing was this 30th day of January 2025 filed via the CM/ECF system and served by electronic mail upon all counsel of record.

/s/ Nathan R. Ring
Nathan R. Ring